vulnerability-status-report-SmartMedic 2.0-Default Detect Version_2022-05-25_093143

SmartMedic 2.0 Default Detect Version

7 Vulnerabilities

Vulnerability	Overall Score	Remediation Status	CWE	Reachable	Exploit	Workaround	Solution
BDSA-2021-0936 (CVE-2021-29428)	3	New	CWE-362, CWE-378, CWE-379	–	–	✓	✓

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Vulnerability Description
Gradle on Unix-like systems is vulnerable to a local privilege escalation issue due to how the system temporary directory can be created with open permissions. The open permissions allow multiple users to create and delete files within the directory, and enable an attacker to perform a privilege escalation attack by quickly deleting and recreating files in the system temporary directory.

BDSA-2019-2976 (CVE-2019-16370)	2	New	CWE-916	–	✓	–	✓

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Vulnerability Description
Gradle uses weak cryptographic hashing algorithm, SHA-1, for signing artifacts. This allows spoofing content and makes the application digest crafted artifacts.

BDSA-2019-1008 (CVE-2019-11065)	4.3	New	CWE-300	–	–	–	✓

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Vulnerability Description
Gradle is vulnerable to man-in-the-middle (MitM) attacks due to downloading resources over an insecure protocol (HTTP).

BDSA-2019-2688 (CVE-2019-15052)	3.4	New	CWE-522	–	✓	–	✓

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Gradle is vulnerable to information disclosure due to the unsafe handling of redirection events whenever a repository is being contacted. An attacker could obtain authentication information by hosting a malicious repository instance. This vulnerability only exists whenever Gradle is using a repository that requires authentication, and that repository redirects Gradle to another host in a manner that is uncontrolled by the user.

	Vulnerability	Overall Score	Remediation Status	CWE	Reachable	Exploit	Workaround	Solution
⌄	**CVE-2020-11979**	5	New		–	–	–	–

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Vulnerability Description
As mitigation for CVE-2020-1945 Apache Ant 1.10.8 changed the permissions of temporary files it created so that only the current user was allowed to access them. Unfortunately the fixcrlf task deleted the temporary file and created a new one without said protection, effectively nullifying the effort. This would still allow an attacker to inject modified source files into the build process.

⌄	**BDSA-2021-2200 (CVE-2021-32751)**	2.7	New	CWE-94	–	–	✓	✓

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Vulnerability Description
Gradle contains an arbitrary code execution vulnerability. This allows a local attacker to include malicious code in `JAVA_OPTS` or `GRADLE_OPTS` that will be executed when the `gradlew`tool is used.

⌄	**BDSA-2021-0920 (CVE-2021-29429)**	1.3	New	CWE-377	–	–	✓	✓

Gradle 4.4.0-rc1
github: gradle/gradle:v4.4.0-RC1

Vulnerability Description
Gradle contains an information disclosure vulnerability due to the downloading of files to the system temporary directory. A local attacker can take advantage of this in order to gain access to sensitive data not intended for them. **Note:** The vendor has stated that if you do not use the `TextResourceFactory` API, you are not vulnerable.